Discrete Mathematics 48 (1984) 253–274
North-Holland

SOLUTIONS PRINCIPALES ET RANG D'UN SYSTÈME D'ÉQUATIONS AVEC CONSTANTES DANS LE MONOÏDE LIBRE

J.P. PECUCHET

Université de Rouen, Faculté des Sciences et des Techniques, BP 67, 76130 Mont-Saint-Aignan, France

Received 14 May 1982
Revised 20 April 1983

We extend Lentin's and Makanin's results concerning the solutions' structure and the rank of a constant free equation to the case of a system of equations with constants.

Nous étendons les résultats de Lentin et de Makanin concernant la structure des solutions et le rang d'une équation sans constantes au cas des systèmes d'équations avec constantes.

Introduction

Les équations dans le monoïde libre interviennent entre autres dans l'étude des systèmes de Lyndenmayer (cf. [17]), dans le problème de l'unification dans les systèmes formels (cf. [6]), dans les problèmes de motifs (cf. [1]) et s'apparentent aux équations dans le groupe libre (cf. [11] et [12]).

Historiquement leur étude a commencé par celle des équations sans constantes [7, 9]. Une telle équation est un couple (e, e') de mots écrits sur un alphabet fini E. Une solution de (e, e') est un morphisme total $\alpha: E^* \to A^*$ (alphabet fini quelconque) vérifiant $\alpha e = \alpha e'$. Le rang de α est le cardinal du plus petit code de A^* sur lequel on puisse écrire les mots de αE, et le rang de l'équation le maximum des rangs de ses solutions. Une seconde solution $\beta: E^* \to B^*$ dérive de α s'il existe un morphisme continu $\theta: A^* \to B^*$ tel que $\beta = \theta\alpha$. La solution α est principale si elle ne dérive que d'elle-même.

Lentin montre qu'une solution dérive d'une unique solution principale (il donne deux méthodes distinctes pour l'obtention de celle-ci) et calcule les solutions et le rang de certains types particuliers d'équations sans constantes [7]. Makanin montre ensuite que l'on peut calculer le rang d'une équation sans constantes, d'abord dans le cas de quatre inconnues [18], puis dans le cas général [14].

L'étude des équations avec constantes fut abordée par Hmelewskii [5]. Une telle équation est un couple (e, e') de mots écrits sur un alphabet fini $\mathscr{E} = E \cup C$ union disjointe de l'alphabet E des inconnues et de l'alphabet C des constantes. Une solution de (e, e') est un morphisme $\alpha: \mathscr{E}^* \to C^*$ fixant les constantes et vérifiant $\alpha e = \alpha e'$. Contrairement à ce qui se passe pour une équation sans

constantes, une telle équation n'a pas toujours de solution. Se pose donc le problème de savoir décider si une équation avec constantes donnée admet ou non une solution. L'étude de cette question est abordée par Hmelewskii qui dans [5] résoud le problème dans le cas de 3 inconnues. Le problème est ensuite résolu dans le cas général par Makanin dans [13].

Afin d'unifier les théories des équations avec et sans constantes nous généralisons la notion jusqu'alors trop restrictive de solution d'une équation avec constantes. Si (e, e') est une équation avec constantes sur l'alphabet $\mathscr{E} = E \cup C$ nous appelons solution tout morphisme continu et fixant les constantes $\alpha: \mathscr{E}^* \to A^*$ vérifiant $\alpha e = \alpha e'$. L'alphabet A sur lequel s'écrit la solution contient l'alphabet C des constantes mais peut être plus grand. Ceci permet d'introduire des notions de rang et de solutions principales qui généralisent celles introduites précédemment pour les seules équations sans constantes. De plus l'alphabet C des constantes pouvant être vide, l'étude des équations sans constantes devient un cas particulier de celle des équations avec constantes. Nous montrons alors que tous les résultats classiques concernant le rang et la structure syntaxique des solutions s'étendent non seulement aux équations mais même aux systèmes quelconques d'équations avec constantes.

En particulier nous montrons que toute solution dérive d'une unique solution principale, généralisant ainsi le résultat de [7]. Puis nous généralisons les résultats de [14] et [15] en montrant que l'on peut calculer le rang d'une quelconque équation. Nous montrons d'ailleurs à ce sujet que les deux algorithmes donnés par Makanin dans [13] et [14] ne sont pas indépendants en montrant que l'on sait calculer le rang dès que l'on sait décider de l'existence d'une solution. Nous terminons cet article en montrant comment l'étude des solutions principales et du rang d'un système fini peut se ramener à celle d'une simple équation, précisant et complétant ainsi un résultat de [5] (on notera à ce sujet que le résultat de [4] montre que tout système algébrique se ramène à l'un de ses sous-systèmes finis).

1. Définitions, notations

Ce chapitre est destiné à introduire les notations, définitions et résultats d'ordre général utilisés par la suite. Nous y donnons également quelques lemmes plus techniques et moins classiques dont nous aurons besoin plus tard.

Nous utiliserons les notations suivantes. Si A est un ensemble quelconque (appelé alphabet), A^* désigne le monoïde libre sur A, 1 le mot vide de A^* et $A^+ = A^* - \{1\}$ le semi-groupe libre sur A. Pour $u \in A^*$ on note $u(n)$ la $n$ième lettre du mot u, $|u|$ la *longueur* de u, $|u|_a$ le nombre d'occurrences de la lettre $a \in A$ dans u et on pose $\text{alph}(u) = \{a \in A \mid |u|_a > 0\}$. Pour $L \subset A^*$ on pose $\text{alph}\, L = \bigcup_{u \in L} \text{alph}(u)$. Pour $X \subset A^*$ et $Y \subset A^*$ on pose $X^{-1}Y = \{v \in A^* \mid \exists u \in X\ uv \in Y\}$ et $YX^{-1} = \{u \in A^* \mid \exists v \in X\ uv \in Y\}$.

Un morphisme $\varphi: A^* \to B^*$ est dit *total* si $\text{alph}(\varphi A) = B$, *continu* si $\varphi A \subset B^+$,

et *litteral* si $\varphi A \subset B$. Soient A_1 et A_2 deux alphabets disjoints, on appelle *projection* de $(A_1 \cup A_2)^*$ sur A_1^* le morphisme $\Pi: (A_1 \cup A_2)^* \to A_1^*$ defini par $\Pi x = x$ si $x \in A_1$ et $\Pi_x = 1$ si $x \in A_2$. On appelle *somme* des morphismes $\alpha_1: A_1^* \to B^*$ et $\alpha_2: A_2^* \to C^*$ le morphisme $\alpha_1 \oplus \alpha_2: (A_1 \cup A_2)^* \to (B \cup C)^*$ defini par $\alpha_1 \oplus \alpha_2 x = \alpha_1 x$ si $x \in A_1$ et $\alpha_1 \oplus \alpha_2 x = \alpha_2 x$ si $x \in A_2$.

On note X^* le sous-monoïde de A^* engendré par une partie X du monoïde libre A^*. On dit qu'un sous-monoïde M de A^* est *libre* s'il existe une partie X de M telle que tout mot de M se factorise de façon unique en mots de X. Ceci signifie que si X^* designe le monoïde libre sur l'alphabet X, l'insertion $\theta: X^* \to A^*$ (définie par $\theta x = x$) est un morphisme injectif. Rappelons (cf. [10]) que l'on a alors $M = X^*$ avec $X = (M-1) - (M-1)^2$. X est appelé la *base* de M et l'on dit que X est un *code*. Pour toute partie Y de A^*, il existe un plus petit sous-monoïde libre M de A^* contenant Y dont la base X est appelée le *noyau libre* de Y et sera notée $X = [Y]$.

En ce qui concerne le noyau libre rappelons les deux résultats suivants (cf. [2]).

Theorème du defaut. *Si X est une partie finie de A^* qui n'est pas un code on a* $\operatorname{card}[X] \leqslant \operatorname{card} X - 1$.

Lemme 1.1. *Si X est une partie de A^* et $M = [X]^*$ on a*

$$[X] \subseteq XM^{-1} \cap M^{-1}X.$$

En ce qui concerne les monoïdes libres et leurs bases nous utiliserons les résultats suivants.

Lemme 1.2. *Un sous-monoïde P de A^* est libre ssi on a*

$$P = P^{-1}P \cap PP^{-1}.$$

Voir la preuve dans [3].

On rappelle egalement que l'image directe ou réciproque d'un code par un morphisme injectif est un code. De même pour l'image réciproque par un morphisme littéral. Rappelons enfin que l'image directe par un morphisme injectif et l'image réciproque par un morphisme quelconque d'un monoïde libre est libre.

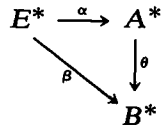
En ce qui concerne le noyau libre de l'image d'un morphisme ón notera le lemme technique suivant.

Lemme 1.3. *Si $\alpha: E^* \to A^*$ et $\theta: A^* \to B^*$ sont deux morphismes on a la formule*: $[\theta\alpha E] = [\theta[\alpha E]]$.

Preuve. On a $\theta\alpha E^* \subset \theta[\alpha E]^* \subset [\theta[\alpha E]]^*$ d'où $[\theta\alpha E]^* \subset [\theta[\alpha E]]^*$. D'autre part $\theta^{-1}([\theta\alpha E]^*)$ est un sous-monoïde libre de A^* contenant αE d'où $[\alpha E]^* \subset \theta^{-1}([\theta\alpha E]^*)$ et donc $\theta[\alpha E]^* \subset [\theta\alpha E]^*$ et finalement $[\theta[\alpha E]]^* \subset [\theta\alpha E]^*$. On a donc $[\theta\alpha E]^* = [\theta[\alpha E]]^*$ d'où le résultat. □

On appelle *rang* d'un morphisme $\alpha: A^* \to B^*$ et on note $\mathrm{rg}\,\alpha$ le cardinal du noyau libre de αA (avec A fini). Le théorème du défaut montre que $\mathrm{rg}\,\alpha \leqslant \mathrm{card}\,A$ avec égalité ssi α est injectif.

Si $\alpha: E^* \to A^*$ et $\beta: E^* \to B^*$ sont deux morphismes on dit respectivement que α *divise*, divise *injectivement*, divise *littéralement* β (noté respectivement $\alpha \leqslant \beta$, $\alpha \leqslant_i \beta$, $\alpha \leqslant_1 \beta$) s'il existe un morphisme $\theta: A^* \to B^*$ respectivement continu, injectif, littéral vérifiant $\beta = \theta\alpha$, c'est-à-dire faisant commuter le diagramme

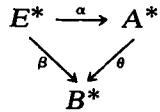


On dit que α et β sont *équivalents* (noté $\alpha \sim \beta$) s'il existe un isomorphisme θ vérifiant $\beta = \theta\alpha$. Alors θ prolonge une bijection de A sur B et β est obtenu à partir de α en renommant les lettres.

Dans ce qui suit nous étudions de plus prêt le rang et la division des morphismes. Nous montrerons d'abord qu'en général le rang diminue par morphisme, mais qu'il est conservé par morphisme injectif. Nous verrons ensuite qu'un morphisme peut en général en diviser un autre de plusieurs façons. Nous préciserons les cas dans lesquels on est assuré de l'unicité et en déduirons que deux morphismes totaux sont équivalents ssi ils se divisent l'un l'autre. Dans les autres cas nous préciserons ce qu'ont de commun les differents morphismes à l'aide desquels un même morphisme peut en diviser un autre.

Proposition 1.4. *Si* $\alpha \leqslant \beta$ *alors* $\mathrm{rg}\,\alpha \geqslant \mathrm{rg}\,\beta$. *Si de plus* $\alpha \leqslant_i \beta$ *on a* $\mathrm{rg}\,\alpha = \mathrm{rg}\,\beta$.

Preuve. Soient α, β, θ des morphismes faisant commuter le diagramme



On a $[\beta E] = [\theta\alpha E] = [\theta[\alpha E]]$ d'après le Lemme 1.3. On en déduit d'après le théorème du défaut

$$\mathrm{rg}\,\beta = \mathrm{card}[\beta E] \leqslant \mathrm{card}\,\theta[\alpha E] \leqslant \mathrm{card}[\alpha E] = \mathrm{rg}\,\alpha.$$

Si de plus $\alpha \leqslant_i \beta$ on peut supposer θ injectif et $\theta[\alpha E]$ est un code. Il vient donc $[\beta E] = \theta[\alpha E]$ d'où $\mathrm{rg}\,\beta = \mathrm{rg}\,\alpha$. □

Remarque 1.5. Si $\alpha \leqslant \beta$ il se peut que α divise β au moyen de plusieurs

morphismes distincts et même de natures distinctes comme le montre l'exemple suivant.

Soient $\alpha: \{x\}^* \to \{a, b, c\}^*$ et $\beta: \{x\}^* \to \{a, b\}^*$ définis par $\alpha x = abc$ et $\beta x = abaab$. α divise β au moyen du morphisme injectif θ défini par $\theta a = ab$, $\theta b = aa$, $\theta c = b$ et du morphisme *non* injectif θ' défini par $\theta' a = a$, $\theta' b = ba$, $\theta' c = ab$.

Les deux résultats suivants montrent que l'unicité est cependant assurée dans le cas de la division littérale.

Lemme 1.6. *Si α et β sont deux morphismes* totaux *et θ un morphisme* continu *vérifiant $\beta = \theta\alpha$ alors θ est littéral ssi $|\alpha x| = |\beta x|$ pour tout $x \in E$.*

Preuve. La condition est évidemment nécessaire. Réciproquement si θ est non littéral, il existe un $a \in A$ tel que $|\theta a| > 1$. α étant total et θ continu on en déduit l'existence d'un $x \in E$ tel que $|\alpha x| > |\beta x|$. □

Proposition 1.7. *Si α et β sont deux morphismes totaux vérifiant $\alpha \leqslant_1 \beta$ alors α divise β au moyen d'un unique morphisme.*

Preuve. Soit $\alpha: E^* \to A^*$ et $\beta: E^* \to B^*$ des morphismes totaux vérifiant $\alpha \leqslant_1 \beta$. Le lemme précédant montre que l'on a $|\alpha x| = |\beta x|$ pour tout $x \in E$ et que tout morphisme continu au moyen duquel α divise β est littéral. Si θ et θ' sont deux tels morphismes et si $a \in A$ la considération d'un $x \in E$ tel que $\alpha x = uav$ (α total) et les égalités $\theta u \theta a \theta v = \theta' u \theta' a \theta' v$ et $|\theta u| = |\theta' u|$ montrent que $\theta a = \theta' a$ d'où $\theta = \theta'$. □

On en déduit la

Proposition 1.8. *Si $\alpha: E^* \to A^*$ et $\beta: E^* \to B^*$ sont deux morphismes totaux on a:*

$$\alpha \leqslant \beta \quad et \quad \beta \leqslant \alpha \quad ssi\ \alpha \sim \beta.$$

Preuve. La réciproque est évidente. Dans l'autre sens soit $\theta: A^* \to B^*$ et $\theta': B^* \to A^*$ des morphismes continus vérifiant $\beta = \theta\alpha$ et $\alpha = \theta'\beta$. Puisque $\theta'\theta$ est continu et que $\alpha \leqslant_1 \alpha$ la Proposition 1.7 montre que $\theta'\theta = \mathrm{id}_{A^*}$ et par symétrie $\theta\theta' = \mathrm{id}_{B^*}$, ce qui montre que θ et θ' sont des isomorphismes réciproques. □

Remarquons qu'un isomorphisme étant à la fois injectif et littéral la proposition précédente reste encore vraie en remplaçant $\leqslant$ par $\leqslant_i$ ou $\leqslant_l$.

On notera enfin que si $\alpha: E^* \to A^*$ divise β à l'aide de θ et θ' alors ces deux morphismes coïncident sur le noyau libre $[\alpha E]$, ce qui est une conséquence facile des deux lemmes suivants dans lesquels on pose pour $Z \subset A^*$, $\mathscr{L}(Z) = Z^{-1}Z \cap ZZ^{-1}$.

Lemme 1.9. *Soit* $[X]$ *le noyau libre de* $X \subset A^*$ *et* $M = [X]^*$. *Soit* $(U_n)_{n\in\mathbb{N}}$ *la suite définie par* $U_0 = X$, $U_{n+1} = \mathscr{L}(U_n^*)$. *Alors* $M = \bigcup_{n\geqslant 0} U_n^*$.

Preuve. Posons $P = \bigcup_{n\geqslant 0} U_n^*$. On a $U_0^* \subseteq M$ et la relation $U_n^* \subseteq M$ implique $U_{n+1} = \mathscr{L}(U_n^*) \subseteq \mathscr{L}(M) = M$. On a donc $U_n^* \subseteq M$ par récurrence d'où $P \subseteq M$.

D'autre part la relation $U_n^* \subset \mathscr{L}(U_n^*)$ montre que $(U_n)_{n\in\mathbb{N}}^*$ est une suite croissante. On en déduit que P est un sous-monoïde de A^* et que $\mathscr{L}(P) = P$. P est donc un sous-monoïde libre de A^* (Lemme 1.2) qui contient X et est contenu dans M. Par minimalité de M on a donc $M = P$. □

Lemme 1.10. *Si deux morphismes* $\alpha, \beta: A^* \to B^*$ *coïncident sur* $X \subset A^*$ *ils coïncident sur son enveloppe libre* $M = [X]^*$.

Preuve. Posons $E = E(\alpha, \beta) = \{u \in A^* \mid \alpha u = \beta u\}$. Il est clair que si deux des trois mots u, v, uv sont dans E, il en est de même du troisième. On en déduit que E est un sous-monoïde de A^* vérifiant $Z \subset E \Rightarrow \mathscr{L}(Z) \subset E$. En reprenant les notations du Lemme 1.9, si $X \subset E$, on a par récurrence $U_n^* \subset E$ pour tout $n \in \mathbb{N}$ d'où $M \subset E$. □

2. Solutions d'un système d'équations; rang

Nous introduisons dans ce chapitre des notions de solutions et de rang des systèmes d'équations avec constantes qui généralisent celles précédemment introduites par Lentin. Le rang d'une solution, qui mesure le nombre de 'paramètres' qui la définissent, est en général distinct du rang du morphisme sous-jacent. Aussi emploierons-nous le terme de rang vrai pour la première notion, réservant celui de rang pour la seule seconde. Nous préciserons enfin les bornes entre lesquelles peuvent varier les rangs et donnerons quelques précisions concernant le rang vrai et la division des solutions.

On appelle *équation* tout triplet $\Gamma = ((e, e'), E, C)$ où (e, e') est un couple de mots du monoïde libre $\mathscr{E}^*$ sur l'alphabet fini $\mathscr{E} = E \cup C$, où E et C sont deux alphabets disjoints. $E = \{x_1, \ldots, x_n\}$ est l'alphabet des *inconnues* et $C = \{c_1, \ldots, c_m\}$ l'alphabet des *constantes*.

On appelle *système* d'équations tout système $S = (\Gamma_i)_{i\in I} = ((e_i, e_i')_{i\in I}, E, C)$ d'équations sur *les mêmes alphabets* E et C. On dira que S est *sans constantes* si $C = \emptyset$ et *avec constantes* si $C \neq \emptyset$.

On appelle *solution* de Γ tout morphisme *total* $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ (avec $\mathscr{A} = A \cup C$ où A est un alphabet disjoint de C) vérifiant $\alpha e = \alpha e'$ et fixant les constantes (c'est à dire $\alpha c = c$ pour tout $c \in C$). α est une *solution* du système S si c'est une solution de chacune des équations Γ_i.

Notons que α étant total et $\mathscr{E}$ fini, on a $\mathscr{A}$ fini. Notons également que si S est *trivial* (c'est-à-dire si $e_i = e_i'$ pour tout i) tout morphisme total $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ fixant

les constantes est une solution, et que si $E = \emptyset$, S admet une solution ssi c'est un système trivial.

On pose dans ce qui suit $\mathscr{E}' = \text{alph } S = \text{alph}\{e_i e_i' \mid i \in I\}$, $E' = E \cap \mathscr{E}'$, $C' = C \cap \mathscr{E}'$, $\mathscr{A}' = \text{alph}(\alpha\mathscr{E}')$, $A' = A \cap \mathscr{A}'$ et $\alpha' : \mathscr{E}'^* \to \mathscr{A}'^*$ le morphisme total obtenu par restriction de α. α' est une solution de système $S' = ((e_i, e_i'), E', C')$. On appelle alors *rang vrai* de α (noté $\text{rgv}\,\alpha$) la quantité définie par

$$\text{rgv}\,\alpha = \text{rg}\,\alpha' - \text{card}\,C'.$$

Puisque le noyau libre de $\alpha'\mathscr{E}'$ contient C', on a $\text{rg}\,\alpha' \geqslant \text{card}\,C'$. Si de plus le système n'est pas trivial, α' n'est pas injectif et on a $\text{rg}\,\alpha' \leqslant \text{card}\,E' + \text{card}\,C' - 1$ d'après le théorème du défaut. D'où la proposition:

Proposition 2.1. *Le rang vrai de toute solution d'un système non trivial S sur l'alphabet $\mathscr{E} = E \cup C = \text{alph}\,S$ vérifie:*

$$0 \leqslant \text{rgv}\,\alpha \leqslant \text{card}\,E - 1.$$

L'alphabet des constantes ne dépendant que du système (et pas de la solution) on déduit de la Proposition 1.4:

Proposition 2.2. *Si α et β sont deux solutions d'un même système on a $\text{rgv}\,\alpha \geqslant \text{rgv}\,\beta$ lorsque $\alpha \leqslant \beta$, avec égalité dès que $\alpha \leqslant_i \beta$.*

Remarque 2.3. On peut avoir $\text{rgv}\,\alpha = \text{rgv}\,\beta$ sans que α divise β au moyen d'un morphisme injectif comme le montre l'exemple de l'équation $((xay, az), \{x, y, z\}, \{a\})$ qui admet les solutions α et β définies par $\alpha x = abc$, $\alpha y = bc$, $\alpha z = bcabc$ et $\beta x = abb$, $\beta y = bb$, $\beta z = bbabb$. On a $\text{rgv}\,\alpha = \text{rgv}\,\beta = 1$ bien que le morphisme (unique car littéral) au moyen duquel α divise β soit défini par $\theta b = \theta c = b$.

Une solution de rang vrai nul n'est rien d'autre qu'une solution $\alpha : \mathscr{E}^* \to C^*$. Pour toute solution $\beta : \mathscr{E}^* \to \mathscr{B}^*$ et tout morphisme $\theta : \mathscr{B}^* \to C^*$ fixant les constantes, $\alpha = \theta\beta$ est une solution de rang vrai nul, d'où Proposition 2.4.

Proposition 2.4. *Un système admet une solution ssi il admet une solution de rang vrai nul.*

On remarquera que c'est sur la recherche de telles solutions qu'est basé l'algorithme de Makanin.

Notons qu'un système sans constantes admet toujours une unique solution de rang vrai nul, la solution triviale $\alpha : E^* \to 1$. Par contre un système avec constantes, s'il admet une solution, peut avoir plusieurs solutions de rang vrai nul.

C'est le cas par exemple de l'équation $((ax, xa)), \{x\}, \{a\})$ qui admet les solutions $\alpha_n : \{a, x\}^* \to a^*$ définies par $\alpha_n x = a^n$ $(n \in \mathbb{N})$.

On appelle enfin *rang du système* S et on note rg S le maximum des rangs vrais de ses solutions (avec la convention rg $S = -1$ s'il n'a pas de solution).

Remarque 2.5. La notion de rang dépend de façon cruciale du choix des alphabets. Ainsi on a: $\mathrm{rg}((ax, xa), \emptyset, \{a, x\}) = -1$; $\mathrm{rg}((ax, xa), \{x\}, \{a\}) = 0$; $\mathrm{rg}((ax, xa), \{a, x\}, \emptyset) = 1$.

Remarque 2.6. Les exemples suivants, dans lesquels $\mathrm{rgv}(\alpha, \Sigma)$ désigne le rang vrai de α considéré comme solution du système Σ, montrent qu'il ne faut pas confondre le rang vrai d'une solution d'un système avec les rangs vrais qu'elle peut prendre lorsqu'elle est considérée comme solution des équations constituant le système.

Exemple 2.1. Le système $S = (\Gamma_1, \Gamma_2)$ défini par $\Gamma_1 = ((axx, yya), \{x, y\}, \{a, b\})$ et $\Gamma_2 = ((xxb, byy), \{x, y\}, \{a, b\})$ admet la solution $\alpha : \{x, y, a, b\}^* \to \{a, b\}^*$ définie par $\alpha x = ba$, $\alpha y = ab$. On a $\mathrm{rgv}(\alpha, S) = 0 < \mathrm{rgv}(\alpha, \Gamma_1) = \mathrm{rgv}(\alpha, \Gamma_2) = 1$.

Exemple 2.2. Le système $S = (\Gamma_1, \Gamma_2)$ défini par $\Gamma_1 = ((ax, xa), \{x, y, z\}, \{a\})$ et $\Gamma_2 = ((xy, zx), \{x, y, z\}, \{a\})$ admet la solution $\alpha : \{x, y, z, a\}^* \to \{a, b\}^*$ définie par $\alpha x = a$, $\alpha y = ba$, $\alpha z = ab$. On a $\mathrm{rgv}(\alpha, \Gamma_1) = 0 < \mathrm{rgv}(\alpha, S) = 1 < \mathrm{rgv}(\alpha, \Gamma_2) = 2$.

Exemple 2.3. Le système $S = (\Gamma_1, \Gamma_2)$ défini par $\Gamma_1 = ((xy, yx), \{x, y, z, t\}, \emptyset)$ et $\Gamma_2 = ((zt, tz), \{x, y, z, t\}, \emptyset)$ admet la solution $\alpha : \{x, y, z, t\}^* \to \{a, b\}^*$ définie par $\alpha x = \alpha y = a$ et $\alpha z = \alpha t = b$. On a $\mathrm{rgv}(\alpha, \Gamma_1) = \mathrm{rgv}(\alpha, \Gamma_2) = 1 < \mathrm{rgv}(\alpha, S) = 2$.

On dispose cependant de la majoration suivante:

Proposition 2.7. *Si α est une solution du système $S = (\Gamma_i)_{i \in I}$ on a* $\mathrm{rgv}(\alpha, S) \leqslant \sum_{i \in I} \mathrm{rgv}(\alpha, \Gamma_i)$.

Preuve. Soit $\alpha : \mathscr{E}^* \to \mathscr{A}^*$ une solution du système $S = (\Gamma_i)_{i \in I}$ avec $\mathscr{E} = E \cup C$ où E et C désignent l'alphabet des inconnues et celui des constantes. Posons $X = \mathrm{alph}\, S$, $X_i = \mathrm{alph}\, \Gamma_i$, $C_i = C \cap X_i$ et $C' = C \cap X$. On a alors $X = \bigcup_{i \in I} X_i$, $C' = \bigcup_{i \in I} C_i$, $\mathrm{rgv}(\alpha, S) = \mathrm{card}[\alpha X] - \mathrm{card}\, C'$ et $\mathrm{rgv}(\alpha, \Gamma_i) = \mathrm{card}([\alpha X_i] - C_i)$.

D'une part l'inclusion $\alpha X \subset [\bigcup_i ([\alpha X_i] - C_i) \cup C']^*$ implique

$$[\alpha X]^* \subset \left[\bigcup_i ([\alpha X_i] - C_i) \cup C' \right]^*.$$

D'autre part les inclusions $\alpha X_i \subset [\alpha X]^*$ et $C' \subset [\alpha X]$ impliquent successivement $[\alpha X_i] \subset [\alpha X]^*$ et $\bigcup_i ([\alpha X_i] - C_i) \cup C' \subset [\alpha X]^*$. D'où l'on déduit:

$$\left[\bigcup_i ([\alpha X_i] - C_i) \cup C'\right]^* \subset [\alpha X]^*.$$

On dispose donc de l'égalité:

$$[\alpha X] = \left[\bigcup_i ([\alpha X_i] - C_i) \cup C'\right].$$

Le théorème du défaut donne donc:

$$\operatorname{card}[\alpha X] \leqslant \sum_i \operatorname{card}([\alpha X_i] - C_i) + \operatorname{card} C',$$

ou encore

$$\operatorname{rgv}(\alpha, S) \leqslant \sum_i \operatorname{rgv}(\alpha, \Gamma_i). \qquad \square$$

Remarquons que l'Exemple 2.3 ci-dessus montre que la majoration ne peut être améliorée.

La considération d'une solution de rang maximum et la Proposition 2.1 fournissent le corollaire suivant:

Proposition 2.8. *Le rang d'un système non trivial $S = (\Gamma_i)_{i \in I}$ à n inconnues vérifie les inégalités:*

$$-1 \leqslant \operatorname{rg} S \leqslant \inf\left(n - 1, \sum_{i \in I} \operatorname{rg} \Gamma_i\right).$$

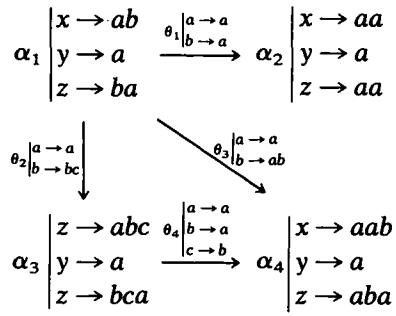
3. Solutions libres, simples

Nous introduisons dans ce paragraphe les notions de solutions libres, simples et principales d'un système d'équations avec constantes. Nous étudions ici les propriétés des solutions libres et des solutions simples et montrons en particulier que toute solution est divisée (moyennant certaines conditions) par une unique solution libre et une unique solution simple. L'étude des solutions principales est reportée au chapitre suivant.

Une solution d'un système S est dite *principale* si toute solution de S qui la divise lui est équivalente. Elle est dite *simple* (*libre*) si toute solution qui la divise injectivement (littéralement) lui est équivalente.

On notera que deux solutions équivalentes sont en même temps toutes deux simples ou libres ou principales.

Exemple 3.1. Considérons l'équation $((xy, yz), \{x, y, z\}, \emptyset)$ dont le schéma suivant représente quatre solutions et les morphismes faisant passer de l'une à l'autre.



On a α_1 principale, α_2 simple et non libre, α_3 libre et non simple, α_4 ni libre ni simple.

Le but de ce paragraphe est de préparer la Proposition 4.6 montrant que toute solution est divisée par une solution principale unique à l'équivalence près. Dans le cas d'une équation ou d'un système fini d'équations ce résultat peut être obtenu de deux façons: soit par l'étude des solutions libres et simples, soit par la décomposition en transformations de Nielsen (voir [7] et [10] pour les équations sans constantes et [16] pour les équations avec constantes). Dans le cas d'un système quelconque nous emploierons la première méthode qui semble ici la plus naturelle.

Nous commencerons par l'étude des solutions libres. Les Propositions 1.6 et 1.7 montrent que pour deux morphismes totaux définis sur $\mathscr{E}^*$ vérifiant $\alpha \leqslant \beta$ on a $\alpha \leqslant_1 \beta$ ssi $|\alpha x| = |\beta x|$ pour tout $x \in \mathscr{E}$, le morphisme continu à l'aide duquel α divise β étant alors unique.

Nous dirons que deux morphismes α et β définis sur le même monoïde libre $\mathscr{E}^*$ ont *même longueur* si $|\alpha x| = |\beta x|$ pour tout $x \in \mathscr{E}$. On a alors $|\alpha u| = |\beta u|$ pour tout $u \in \mathscr{E}^*$. Cette relation est une équivalence sur la classe des morphismes totaux définis sur $\mathscr{E}^*$, moins fine que l'équivalence $\sim$.

Soit F une classe modulo cette équivalence. Alors l'entier $N = \sum_{x \in \mathscr{E}} |\alpha x|$ est indépendant du morphisme $\alpha \in F$ et si $w \in \mathscr{E}^*$ est un mot contenant une fois et une seule chaque lettre de $\mathscr{E}$ on a $|\alpha w| = N$ pour tout $\alpha \in F$.

Soit $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ un élément de F et Π_α l'équivalence définie sur l'intervalle $[N] = [1, N]$ par $(s, t) \in \Pi_\alpha$ ssi $(\alpha w)(s) = (\alpha w)(t)$. En notant $s \mapsto \bar{s}$ la surjection canonique de $[N]$ sur le quotient $[N]/\Pi_\alpha$ la bijection $\theta: [N]/\Pi_\alpha \to \mathscr{A}$ définie par $\bar{s} \mapsto (\alpha w)(s)$ montre que α est équivalent au morphisme $\bar{\alpha}: \mathscr{E}^* \to ([N]/\Pi_\alpha)^*$ défini par $\bar{\alpha} = \theta^{-1}\alpha$. Le quotient $F/\sim$ est donc en bijection naturelle avec l'ensemble des équivalences définies sur $[N]$. Si α et β sont deux éléments de F on vérifie facilement que $\alpha \leqslant_1 \beta$ ssi $\Pi_\alpha \subseteq \Pi_\beta$, l'unique morphisme littéral $\bar{\lambda}: ([N]/\Pi_\alpha)^* \to ([N]/\Pi_\beta)^*$ au moyen duquel $\bar{\alpha}$ divise $\bar{\beta}$ étant alors défini par $\bar{s} \mapsto \bar{\bar{s}}$.

Soit alors $S = ((e_i, e'_i)_{i \in I}, E, C)$ un système sur l'alphabet $\mathscr{E} = E \cup C$, $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ une solution de S vérifiant $|\alpha w| = N$ et $L = \{\beta \mid \beta$ solution de S et $\beta \leqslant_1 \alpha\}$. L est alors une partie de F.

Pour tout $i \in I$ soit $N_i = |\alpha e_i| = |\alpha e'_i|$ et $\sigma_i: [N_i] \to [N]$ l'application définie de la

façon suivante. Si $s \in [N_i]$, soit $x \in \text{alph } e_i$ une lettre vérifiant $e_i = uxv$ $(u, v \in \mathscr{E}^*)$ et $|\alpha u| < s \leqslant |\alpha u| + |\alpha x|$ et soit $t = |\alpha u| + |\alpha x| - s + 1$ (la lettre $(\alpha e_i)(s)$ correspondant ainsi à la lettre $(\alpha x)(t)$ dans le mot αe_i). $\sigma_i s$ est alors défini comme la position occupée par l'occurrence $(\alpha x)(t)$ dans le mot αw.

Le remplacement de e_i par e_i' fournit de la même façon une application $\sigma_i' : [N_i] \to [N]$.

Exemple. Pour l'équation $((xay, ybz), \{x, y, z\}, \{a, b\})$ on peut prendre $w = xyzab$. Pour la solution α définie par $\alpha x = cbb$, $\alpha y = cbbac$, $\alpha z = bac$ on a $N = 13$, $N_1 = 9$, σ_1 et σ_1' étant définis par le tableau suivant.

	1	2	3	4	5	6	7	8	9
σ_1	1	2	3	12	4	5	6	7	8
σ_1'	4	5	6	7	8	13	9	10	11

La définition de σ_i et σ_i' ne faisant intervenir que la longueur des mots de $\alpha\mathscr{E}$ on peut dans cette définition remplacer α par n'importe quel élément $\beta \in F$. Ceci montre qu'un morphisme $\beta \in F$ est solution de S ssi pour tout $i \in I$ et tout $s \in [N_i]$ on a $(\alpha w)(\sigma_i s) = (\alpha w)(\sigma_i' s)$, c'est-à-dire ssi Π_β contient la relation $R = \bigcup_{i \in I} (\sigma_i \times \sigma_i')([N_i])$ où $\sigma_i \times \sigma_i' : [N_i] \to [N] \times [N]$ est définie par $s \mapsto (\sigma_i s, \sigma_i' s)$.

On en déduit donc l'égalité $L = \{\beta \in F \mid R \subseteq \Pi_\beta \subseteq \Pi_\alpha\}$.

Si Π désigne l'équivalence sur $[N]$ engendrée par R on a $R \subseteq \Pi \subseteq \Pi_\beta \subseteq \Pi_\alpha$ pour tout $\beta \in L$. Si $\gamma \in F$ est un morphisme vérifiant $\Pi = \Pi_\gamma$ on en déduit donc que γ est une solution libre de S divisant littéralement toute solution $\beta \in L$ (et en particulier α). De plus toute autre solution libre divisant littéralement α étant divisée par γ lui est équivalente. D'où la

Proposition 3.2. *Toute solution α d'un système S est divisée littéralement par une solution libre γ, unique à un isomorphisme près, et vérifiant la propriété universelle suivante: pour toute solution β vérifiant $\beta \leqslant_1 \alpha$, on a $\gamma \leqslant_1 \beta$ et γ divise β au moyen d'un unique morphisme.*

Cette solution γ sera appelée *solution libre associée à* α et notée $\gamma = l(\alpha)$.

Remarque 3.3. Pour un système fini le résultat est effectif puisque l'on peut alors calculer R et Π et définir $l(\alpha)$: $\mathscr{E}^* \to ([N]/\Pi)^*$ par $l(\alpha)x = \overline{(\alpha x)(1)} \cdots \overline{(\alpha x)(|\alpha x|)}$.

Remarque 3.4. Dans l'Exemple 3.1 on a $l(\alpha_4) = \alpha_3$. α_4 est également divisée par la solution libre $\alpha_1 = l(\alpha_2)$, mais pas littéralement.

Remarque 3.5. Le fait pour une solution d'être libre est une propriété relative à

l'équation. Ainsi la solution α_2 de l'Exemple 3.1 n'est pas une solution libre de l'équation considérée, bien qu'elle soit libre en tant que solution de l'équation $((xz, yxy), \{x, y, z\}, \emptyset)$. Nous allons voir maintenant qu'il en est tout autrement pour les solutions simples.

L'étude des solutions simples repose sur le résultat suivant montrant que le fait d'être simple est une propriété du morphisme indépendante de l'équation.

Proposition 3.6. *Une solution $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ d'un système S est simple ssi $[\alpha\mathscr{E}] = \mathscr{A}$.*

Preuve. Supposons α simple. L'écriture des mots de $\alpha\mathscr{E}$ sur le code $[\alpha\mathscr{E}]$ considéré comme un alphabet fournit une solution $\bar{\alpha}: \mathscr{E}^* \to [\alpha\mathscr{E}]^*$ de S divisant α au moyen de l'insertion $\tau: [\alpha\mathscr{E}]^* \to \mathscr{A}^*$. α étant simple et τ injectif, on a $\bar{\alpha} \sim \alpha$ et τ définit une bijection de $[\alpha\mathscr{E}]$ sur $\mathscr{A}$ (cf. Proposition 1.7) d'où $[\alpha\mathscr{E}] = \mathscr{A}$.

Réciproquement si α vérifie $[\alpha\mathscr{E}] = \mathscr{A}$ et est divisée par $\beta: \mathscr{E}^* \to \mathscr{B}^*$ au moyen du morphisme injectif $\theta: \mathscr{B}^* \to \mathscr{A}^*$ on a $\theta[\beta\mathscr{E}] = [\alpha\mathscr{E}] = \mathscr{A}$ (Lemme 1.3), ce qui montre que θ est un isomorphisme. On a donc $\beta \sim \alpha$ et α simple. □

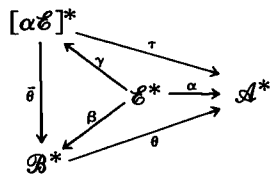
La définition du rang vrai d'une solution et le Lemme 1.10 fournissent immédiatement les deux corollaires suivants:

Proposition 3.7. *Le rang vrai d'une solution simple $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ d'un système $S = ((e_i, e_i')_{i \in I}, E, C)$ sur l'alphabet $\mathscr{E} = E \cup C = \text{alph } S$* est donné par:

$$\text{rgv } \alpha = \text{card } \mathscr{A} - \text{card } C.$$

Proposition 3.8. *Si une solution simple divise une autre solution elle le fait au moyen d'un unique morphisme.*

Soit alors $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ une solution quelconque d'un système S et $\gamma: \mathscr{E}^* \to [\alpha\mathscr{E}]^*$ la solution obtenue à partir de α en écrivant les mots de $\alpha\mathscr{E}$ sur le code $[\alpha\mathscr{E}]$ considéré comme un alphabet. Cette solution est simple d'après la Proposition 3.6 et divise injectivement α à l'aide de l'insertion $\tau: [\alpha\mathscr{E}]^* \to \mathscr{A}^*$.



Si $\beta: \mathscr{E}^* \to \mathscr{B}^*$ est une autre solution divisant injectivement α au moyen du morphisme injectif $\theta: \mathscr{B}^* \to \mathscr{A}^*$ on a $\theta[\beta\mathscr{E}] = [\alpha\mathscr{E}]$ (Lemme 1.3). θ définit donc une bijection de $[\beta\mathscr{E}]$ sur $[\alpha\mathscr{E}]$ dont la réciproque permet de définir un mor-

phisme injectif $\bar{\theta}: [\alpha\mathscr{E}]^* \to \mathscr{B}^*$ vérifiant $\theta\bar{\theta} = \tau$. On a donc $\alpha = \theta\bar{\theta}\gamma = \theta\beta$ d'où $\beta = \bar{\theta}\gamma$ et $\gamma \leqslant_i \beta$.

Enfin toute autre solution simple divisant injectivement α étant divisée par γ lui est équivalente.

Ce qui précède, joint à la Proposition 3.8 nous permet d'énoncer la:

Proposition 3.9. *Toute solution α d'un système S est divisée injectivement par une solution simple γ, unique à un isomorphisme près, et vérifiant la propriété universelle suivante: pour toute solution β vérifiant $\beta \leqslant_i \alpha$, on a $\gamma \leqslant_i \beta$ et γ divise β au moyen d'un unique morphisme.*

Cette solution γ sera appelée *solution simple associée à* α et notée $\gamma = s(\alpha)$.

Remarque 3.10. L'algorithme de calcul du noyau libre d'une partie finie (cf. [2]) pernet de calculer effectivement $s(\alpha)$ pour toute solution α.

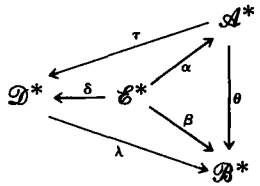
Remarque 3.11. Dans l'Exemple 3.1 la solution $\alpha_2 = s(x_2)$ est simple. Elle est également divisée par la solution simple α_1, mais pas injectivement.

Remarque 3.12. Pour toute solution α on a $\operatorname{rgv} s(\alpha) = \operatorname{rgv} \alpha$ et $\operatorname{rgv} l(\alpha) \geqslant \operatorname{rgv} \alpha$ (Proposition 1.4). Dans l'Exemple 3.1 on a $\operatorname{rgv} l(\alpha_2) = \operatorname{rgv} \alpha_1 = 2 > \operatorname{rgv} \alpha_2 = 1$.

3. Solutions principales

Nous allons prouver l'analogue des Propositions 3.2 et 3.9 dans le cas des solutions principales. Pour cela nous utiliserons les lemmes suivants.

Lemme 4.1. *Soient $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ et $\beta: \mathscr{E}^* \to \mathscr{B}^*$ deux solutions d'un système S. Si α divise β au moyen du morphisme continu θ, il existe une solution $\delta: \mathscr{E}^* \to \mathscr{D}^*$, un morphisme injectif $\tau: \mathscr{A}^* \to \mathscr{D}^*$ pour lequel toute lettre de $\mathscr{D}$ apparait une et une seule fois dans $\tau\mathscr{A}$ et un morphisme littéral $\lambda: \mathscr{D}^* \to \mathscr{B}^*$ faisant commuter le diagramme:*

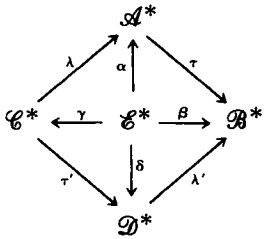


Preuve. Soit C l'alphabet des constantes de S ($\mathscr{E} = E \cup C$). Si $\mathscr{A} = A \cup C$ (union disjointe) soit $\mathscr{D} = D \cup C$ où D est un alphabet disjoint de C de cardinal $|D| = \sum_{a \in A} |\theta a|$. Soit $\tau: \mathscr{A}^* \to \mathscr{D}^*$ le morphisme fixant les constantes, vérifiant

$|\tau a| = |\theta a|$ pour tout $a \in A$ et pour lequel chaque lettre de $\mathscr{D}$ figure une et une seule fois dans les mots de $\tau\mathscr{A}$ (τ est obtenu à partir de θ en fixant les constantes et en distinguant toutes les occurrences de lettres dans les mots θa ($a \in A$)). Soit $\lambda: \mathscr{D}^* \to \mathscr{B}^*$ le morphisme obtenu en envoyant chaque lettre $d \in D$ sur la lettre qu'elle a remplacé dans les mots de $\theta\mathscr{A}$. Il est clair que $\theta = \lambda\tau$, que λ est littéral et τ injectif ($\tau\mathscr{A}$ est bipréfixe). Enfin puisque τ est total et fixe les constantes le morphisme $\delta = \tau\beta: \mathscr{C}^* \to \mathscr{D}^*$ est une solution de S. □

Lemme 4.2. *Soit α et β deux solutions d'un système S vérifiant $\alpha \leqslant_i \beta$. Si β est libre, α l'est aussi.*

Preuve.



Soit $\tau: \mathscr{A}^* \to \mathscr{B}^*$ le morphisme injectif à l'aide duquel $\alpha: \mathscr{C}^* \to \mathscr{A}^*$ divise $\beta: \mathscr{C}^* \to \mathscr{B}^*$ et soit $\gamma: \mathscr{C}^* \to \mathscr{C}^*$ une solution de S divisant α à l'aide du morphisme littéral λ.

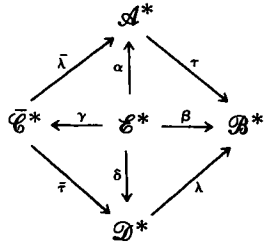
Puisque γ divise β à l'aide de $\tau\lambda$, on peut d'après le Lemme 4.1 fermer le diagramme ci-dessus à l'aide d'une solution δ, d'un morphisme continu τ' et d'un morphisme littéral λ'. Puisque $\delta \leqslant_l \beta$ on a $\delta \sim \beta$ et λ' est donc un isomorphisme. On en déduit que $\tau\lambda = \lambda'\tau'$ et aussi λ sont injectifs. Mais λ étant littéral, injectif et total, est un isomorphisme d'où $\gamma \sim \alpha$, ce qui montre que α est libre. □

Remarque 4.3. α libre n'implique pas β libre comme le montre le cas des solutions α_1 et α_4 de l'Exemple 3.1.

On dispose cependant du résultat suivant:

Lemme 4.4. *Soient $\alpha: \mathscr{C}^* \to \mathscr{A}^*$ et $\beta: \mathscr{C}^* \to \mathscr{B}^*$ deux solutions d'un système S vérifiant $\alpha \leqslant_i \beta$. Si α est libre et divise β au moyen d'un morphisme injectif $\tau: \mathscr{A}^* \to \mathscr{B}^*$ pour lequel toute lettre de $\mathscr{B}$ figure une et une seule fois dans $\tau\mathscr{A}$, alors β est libre.*

Preuve.



Soit $S = ((e_i, e'_i)_{i\in I}, E, C)$ et $\mathscr{C} = E \cup C$. Soit $\delta: \mathscr{C}^* \to \mathscr{D}^*$ une solution de S divisant β au moyen du morphisme littéral $\lambda: \mathscr{D}^* \to \mathscr{B}^*$.

Soit $\mathscr{C} = \lambda^{-1}(\tau\mathscr{A})$ l'ensemble des mots $w \in \mathscr{D}^*$ pour lesquels il existe un $a \in \mathscr{A}$ tel que $\lambda w = \tau a$. $\mathscr{C}$ étant l'image réciproque d'un code par un morphisme littéral est un code et on a évidemment $C \subset \mathscr{C}$.

Soit $\bar{\mathscr{C}}$ un alphabet contenant C et en bijection avec $\mathscr{C}$ par l'application $w \mapsto \bar{w}$ de $\mathscr{C}$ dans $\bar{\mathscr{C}}$ (avec $\bar{c} = c$ pour tout $c \in C$). Soit $\bar{\lambda}: \bar{\mathscr{C}}^* \to \mathscr{A}^*$ le morphisme littéral défini par $\bar{\lambda}\bar{w} = b$ ssi $\tau b = \lambda w$ et $\bar{\tau}: \bar{\mathscr{C}}^* \to \mathscr{D}^*$ le morphisme injectif défini par $\bar{\tau}\bar{w} = w$.

On a évidemment $\tau\bar{\lambda} = \lambda\bar{\tau}$.

D'autre part puisque $\lambda\delta\mathscr{E}^* = \tau\alpha\mathscr{E}^* \subset \tau\mathscr{A}^*$ on a $\delta\mathscr{E}^* \subset \mathscr{C}^*$ et tout mot de $\delta\mathscr{E}$ s'écrit de façon unique sur le code $\mathscr{C}$. Soit donc $\gamma: \mathscr{E}^* \to \bar{\mathscr{C}}^*$ le morphisme défini par $\gamma x = \bar{w}_1 \cdots \bar{w}_n$ ssi $\delta x = w_1 \cdots w_n$ $(w_i \in \mathscr{C})$.

Il est clair que γ est total et est une solution de S vérifiant $\bar{\lambda}\gamma = \alpha$ et $\bar{\tau}\gamma = \delta$. On a donc $\gamma \leqslant_1 \alpha$ d'où $\gamma \sim \alpha$ et $\bar{\lambda}$ est un isomorphisme. On en déduit que $\lambda\bar{\tau} = \tau\bar{\lambda}$ est injectif.

Montrons que ceci implique que λ est lui-même injectif. Puisque δ est total et que $\delta\mathscr{E} \subset \mathscr{C}^*$, toute lettre $d \in \mathscr{D}$ apparait dans un mot de $\mathscr{C}$. Soient alors $d, d' \in \mathscr{D}$ telles que $\lambda d = \lambda d'$ et soient w, $w' \in \mathscr{C}$ tels que $w = udv$ et $w' = u'd'v'$ $(u, v, u', v' \in \mathscr{D}^*)$. On a alors $\lambda\bar{\tau}\bar{w} = \lambda u\lambda d\lambda v = \tau\bar{\lambda}\bar{w} \in \tau\mathscr{A}^*$ et $\lambda\bar{\tau}\bar{w}' = \lambda u'\lambda d'\lambda v' = \tau\bar{\lambda}\bar{w}' \in \tau\mathscr{A}^*$. Mais la lettre $\lambda d = \lambda d' \in \mathscr{B}$ apparait une et une seule fois dans $\tau\mathscr{A}$. On a donc $\lambda\bar{\tau}\bar{w} = \lambda\bar{\tau}\bar{w}'$ et $\lambda u = \lambda' u$. On en déduit $w = w'$ ($\lambda\bar{\tau}$ et $\bar{\tau}$ injectifs) et $|u| = |u'|$ d'où $d = d'$.

λ est donc injectif, littéral et total et par conséquence bijectif, ce qui montre que $\delta \sim \beta$ et que β est libre. □

Lemme 4.5. *Une solution est principale ssi elle est à la fois libre et simple.*

Preuve. La condition est évidemment nécessaire. Réciproquement si une solution $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ divise une solution libre et simple $\beta: \mathscr{E}^* \to \mathscr{B}^*$ à l'aide d'un morphisme θ on dispose d'après le Lemme 4.1 d'une solution $\delta: \mathscr{E}^* \to \mathscr{D}^*$ vérifiant

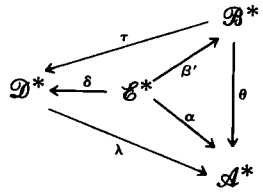
$\alpha \leqslant_i \delta \leqslant_l \beta$. Puisque β est libre on a $\delta \sim \beta$. δ comme β est donc simple, d'où $\alpha \sim \delta$, et finalement $\alpha \sim \beta$, ce qui montre que β est principale. □

Nous pouvons maintenant énoncer la:

Proposition 4.6. *Toute solution α d'un système S est divisée par une solution principale β unique à un isomorphisme près. β est définie par $\beta = s(l(\alpha))$ et vérifie la propriété universelle suivante: pour toute solution γ de S vérifiant $\gamma \leqslant \alpha$ on a $\beta \leqslant \gamma$ et β divise γ à l'aide d'un unique morphisme.*

Preuve. On a évidemment $\beta = s(l(\alpha)) \leqslant \alpha$. D'autre part $s(l(\alpha))$ est simple et vérifie $s(l(\alpha)) \leqslant_i l(\alpha)$. β est donc également libre d'après le Lemme 4.2 et donc principale d'après le Lemme 4.5.

Réciproquement soit β': $\mathscr{E}^* \to \mathscr{B}^*$ une solution principale divisant α: $\mathscr{E}^* \to \mathscr{A}^*$ à l'aide du morphisme continu θ. D'après le Lemme 4.1 on dispose d'une solution δ: $\mathscr{E}^* \to \mathscr{D}^*$, d'un morphisme injectif τ: $\mathscr{B}^* \to \mathscr{D}^*$ pour lequel toute lettre de $\mathscr{D}$ apparait une et une seule fois dans $\tau\mathscr{B}$ et d'un morphisms littéral λ: $\mathscr{D}^* \to \mathscr{A}^*$ faisant commuter le diagramme



δ est alors libre d'après le Lemme 4.4 et donc $\delta \sim l(\alpha)$. On en déduit $\beta = s(l(\alpha)) \leqslant_i \beta'$ d'où $\beta' \sim \beta$.

Enfin si une solution γ divise α on a d'après ce qui précède $\beta' = s(l(\gamma)) \leqslant \alpha$ avec β' principale d'où $\beta \sim \beta'$ et donc $\beta \leqslant \gamma$. □

Cette solution $\beta = s(l(\alpha))$ sera appelée *solution principale associée à α* et notée $\beta = p(\alpha)$.

Remarque 4.7. Les Remarques 3.3 et 3.10 permettent le calcul effectif de $s(l(\alpha))$ lorsque le système est fini.

Remarque 4.8. Un morphisme α étant solution du système $S = (\Gamma_i)_{i \in I}$ ssi c'est une solution de chacune des équations Γ_i, pour que α soit une solution principale de S il suffit qu'elle soit solution de chacune des Γ_i et solution principale d'au moins une équation Γ_i.

La condition n'est cependant pas nécessair comme le montre l'exemple du

système $S = (\Gamma_1, \Gamma_2)$ avec $\Gamma_1 = ((xy, zt), \{x, y, z, t\}, \emptyset)$ et $\Gamma_2 = ((xx, z), \{x, y, z, t\}, \emptyset)$.

Une solution principale du système est donnée par $\alpha x = x$, $\alpha y = xt$, $\alpha z = xx$, $\alpha t = t$. La solution principale de Γ_1 associée à α est donnée par $\alpha_1 x = x$, $\alpha_1 y = zt$, $\alpha_1 z = xz$, $\alpha_1 t = t$. La solution principale de Γ_2 associée à α est donnée par $\alpha_2 x = x$, $\alpha_2 y = y$, $\alpha_2 z = xx$, $\alpha_2 t = t$. On a ici $\alpha_1 \neq \alpha$ et $\alpha_2 \neq \alpha$.

Puisque $\alpha \leqslant \beta$ implique $\mathrm{rgv}\,\alpha \geqslant \mathrm{rgv}\,\beta$ on déduit immédiatement de la Proposition 4.6. 1a

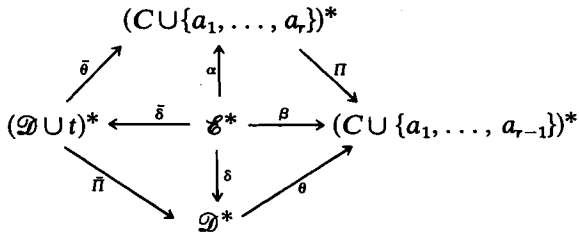
Proposition 4.9. *Le rang d'un système S est égal au maximum des rangs vrais de ses solutions principales.*

Le lemme suivant montre qu'en fait un système admet des solutions principales à tous les rangs.

Lemme 4.10. *Si $\alpha: \mathscr{E}^* \to (C \cup \{a_1, \ldots, a_r\})^*$ est une solution principale et si Π est la projection de $(C \cup \{a_1, \ldots, a_r\})^*$ sur $(C \cup \{a_1, \ldots, a_{r-1}\})^*$ alors $\beta = \Pi\alpha$ est encore une solution principale.*

Preuve. Le Lemme 1.3 et la Proposition 3.6 donnent $[\beta\mathscr{E}] = [\Pi(C \cup \{a_1, \ldots, a_r\})] = C \cup \{a_1, \ldots, a_{r-1}\}$ et donc β est simple.

Montrons qu'elle est également libre. Soit $\delta: \mathscr{E}^* \to \mathscr{D}^*$ une solution divisant β au moyen du morphisme littérat θ. Soit $t \notin \mathscr{D}$, $\bar{\Pi}$ la projection de $(\mathscr{D} \cup t)^*$ sur $\mathscr{D}^*$ et $\bar{\theta}: (\mathscr{D} \cup t)^* \to (C \cup \{a_1, \ldots, a_r\})^*$ le morphisme défini par $\bar{\theta} y = \theta y$ si $y \in \mathscr{D}$ et $\bar{\theta} t = a_r$.



Pour $x \in E$, soit $\alpha x = u_1 a_r u_2 a_r \cdots u_p a_r u_{p+1}$ $(p \in \mathbb{N})$ la factorisation de αx selon les occurrences de a_r, c'est-à-dire l'unique factorisation de αx pour laquelle $u_i \in (C \cup \{a_1, \ldots, a_{r-1}\})^*$ pour tout $1 \leqslant i \leqslant p+1$. On a alors $\beta x = u_1 \cdots u_{p+1}$ et θ étant littéral, il existe une unique factorisation de δx en $\delta x = v_1 \cdots v_{p+1}$ vérifiant $\theta v_i = u_i$ pour $1 \leqslant i \leqslant p+1$ (l'unicité est assurée par les conditions: $|v_i| = |u_i|$). Posons $\bar{\delta} x = v_1 t v_2 \cdots v_p t v_{p+1}$. On a alors $\bar{\Pi}\bar{\delta} x = \delta x$ et $\bar{\theta}\bar{\delta} x = \alpha x$. Pour $c \in C$ posons $\bar{\delta} c = c$. On définit ainsi un morphisme $\bar{\delta}: \mathscr{E}^* \to (\mathscr{D} \cup t)^*$ fixant les constantes et vérifiant $\bar{\Pi}\bar{\delta} = \delta$ et $\bar{\theta}\bar{\delta} = \alpha$. D'autre par une récurrence sur la longueur du mot $w \in \mathscr{E}^*$ montre que pout tout mot $w \in \mathscr{E}^*$, si $\alpha w = u_1 a_r \cdots u_p a_r u_{p+1}$ est la factorisation de αw selon les ocurrences de a_r et si $\delta w = v_1 \cdots v_{p+1}$ est la factorisation

de δw vérifiant $\theta v_i = u_i$ $(1 \leqslant i \leqslant p+1)$ alors $\bar{\delta} w$ est donné par $\bar{\delta} w = u_1 t \cdots u_p t u_{p+1}$. En particulier $\alpha w = \alpha w'$ implique $\bar{\delta} w = \bar{\delta} w'$. On en déduit donc que $\bar{\delta}$ est, comme α, une solution de S. Mais c'est une solution divisant la solution principale α. On en déduit donc que $\bar{\theta}$ et aussi θ sont des isomorphismes, d'où $\delta \sim \beta$. β est donc libre, mais aussi simple et donc principale. □

La Proposition 4.9 et le Lemme 4.10 fournissent donc immédiatement la

Proposition 4.11. *Un système de rang $r \geqslant 0$ admet au-moins une solution principale de rang vrai ρ pour tout $0 \leqslant \rho \leqslant r$.*

5. Calcul du rang

Nous nous proposons de montrer ici que tout algorithme décidant de l'existence d'une solution d'une équation avec constantes (par exemple l'algorithme de Makanin) permet de calculer le rang d'une équation quelconque (avec ou sans constantes), ce qui généralise le résultat obtenu par Makanin dans [14]. Nous étendrons ensuite le résultat aux systèmes finis.

Soit donc $\Gamma = ((e, e'), E, C)$ une équation sur l'alphabet non vide $\mathscr{E} = \text{alph}\, ee' = E \cup C$. Si $E = \emptyset$, il est clair que l'équation est de rang 0 ou -1 suivant qu'elle est ou non triviale. Si d'autre part l'équation est triviale $(e = e')$, il est clair que son rang est donné par $\text{rg}\, \Gamma = \text{card}\, E$. Nous supposerons donc dans la suite $e \neq e'$ et $E \neq \emptyset$. Nous poserons $E = \{x_1, \ldots, x_{n+1}\}$ $(n \geqslant 0)$ et $C = \{c_1, \ldots, c_m\}$ $(m \geqslant 0$, avec la convention $n = 0$ si $C = \emptyset)$. Nous utiliserons les deux lemmes suivants:

Lemme 5.1. *Si $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ est une solution principale de Γ toute lettre de $\mathscr{A}$ est initiale (et finale) d'un mot de $\alpha\mathscr{E}$.*

Preuve. α étant principale, d'après la Proposition 3.6, $\mathscr{A}$ est le noyau libre de $\alpha\mathscr{E}$. D'après le Lemme 1.1, toute lettre de $\mathscr{A}$ est donc à la fois initiale et finale d'un mot de $\alpha\mathscr{E}$. □

Notons que cette propriété ne caractérise pas les solutions principales comme le montre α_2 dans l'Exemple 3.1. On peut cependant obtenir un renseignement sur le rang d'une équation admettant une telle solution par le:

Lemme 5.2. *Si Γ admet une solution $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ pour laquelle toute lettre de $\mathscr{A} = A \cup C$ (union disjointe) est initiale d'un mot de $\alpha\mathscr{E}$ on a* $\text{rang}\, \Gamma \geqslant \text{card}\, A$.

Preuve. Soit $\beta: \mathscr{E}^* \to \mathscr{B}^*$ la solution principale associé à α et $\theta: \mathscr{B}^* \to \mathscr{A}^*$ le morphisme continu vérifiant $\alpha = \theta\beta$.

Soit $k = \text{card}\, A$ avec $A = \{a_1, \ldots, a_k\}$. Soient $\alpha\varepsilon_1, \ldots, \alpha\varepsilon_{k+m}$ $(\varepsilon_i \in \mathscr{E})$ des mots de $\alpha\mathscr{E}$ commençant respectivement par les lettres $a_1, \ldots, a_k$, $c_1, \ldots, c_m$. La relation $\alpha = \theta\beta$ implique que les mots $\beta\varepsilon_1, \ldots, \beta\varepsilon_{k+m}$ commencent tous par une lettre différente et donc que $\text{card}\, \beta \geqslant k+m$ d'où $\text{rgv}\, \beta = \text{card}\, \mathscr{B} - \text{card}\, C \geqslant k$. Mais le rang de Γ étant le maximum des rangs vrais de ses solutions principales on a $\text{rang}\, \Gamma \geqslant k$. □

Voyons maintenant comment ces deux lemmes permettent de calculer le rang de l'équation Γ. Considérons un alphabet $A = \{a_1, \ldots, a_n\}$ disjoint de $\mathscr{E}$. Nous poserons $A_r = \{a_1, \ldots, a_r\}$ et $\mathscr{E}_r = \mathscr{E} \cup A_r$ $(0 \leqslant r \leqslant n)$ avec $A_0 = \emptyset$. Nous introduirons les définitions suivantes: nous appellerons substitution initiale tout morphisme $\varphi: \mathscr{E}^* \to \mathscr{E}_r^*$ $(0 \leqslant r \leqslant n)$ obtenu, à partir d'une application $X: E \to A_r \cup 1$ vérifiant $A_r \subset XE$, par les égalités: $\forall c \in C\ \varphi c = c$ et $\forall x \in E\ \varphi x = (Xx)x$. Nous dirons qu'une équation $\Gamma' = ((f, f'), E, C \cup A_r)$ sur l'alphabet $\mathscr{E}_r$ est associée à Γ s'il existe une substitution initiale $\varphi: \mathscr{E}^* \to \mathscr{E}_r^*$ pour laquelle on ait $(f, f') = (\varphi e, \varphi e')$. Le calcul du rang de Γ se déduit alors immédiatement de la proposition suivante:

Proposition 5.3. *Si l'équation Γ est de rang r $(0 \leqslant r \leqslant n)$, il existe une équation Γ' sur $\mathscr{E}_r$ associé à Γ qui admette une solution. Réciproquement, s'il existe une équation Γ' sur $\mathscr{E}_r$ $(0 \leqslant r \leqslant n)$ associée à Γ qui admette une solution, l'équation Γ est de rang supérieur ou égal à r.*

Preuve. Supposons Γ de rang r et soit $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ une solution principale de Γ de rang vrai r. Puisque $\text{card}\, \mathscr{A} = m + r$ et que α n'est définie qu'à un isomorphisme près, on peut supposer $\mathscr{A} = C \cup A_r$. Soit $X: E \to (A_r \cup 1)$ l'application définie par $Xx = 1$ si $\alpha x = 1$ et $Xx = a$ si $\alpha x \in aA_r^*$. α étant principale, on a $A_r \subset XE$ d'après le Lemme 5.1. Soit donc $\varphi: \mathscr{E}^* \to \mathscr{E}_r^*$ la substitution initiale déduite de X et soit $\Gamma' = ((f, f'), E, C \cup A_r)$ l'équation sur $\mathscr{E}_r$ associée à Γ par φ. Alors Γ' admet une solution. Soit en effet $\gamma: \mathscr{E}_r^* \to \mathscr{A}^*$ le morphisme fixant les éléments de $\mathscr{A} = C \cup A_r$ et vérifiant: $\forall x \in E\ \gamma x = u \in \mathscr{A}^*$ ssi $\alpha x = (Xx)u$. Alors γ est total et on a de façon évidente $\gamma f = \gamma\varphi e = \alpha e$ et $\gamma f' = \gamma\varphi e' = \alpha e'$ d'où $\gamma f = \gamma f'$, ce qui montre que γ est une solution de Γ'.

Réciproquement, soit $\Gamma' = ((f, f'), E, C \cup A_r)$ une équation sur $\mathscr{E}_r$ $(0 \leqslant r \leqslant n)$ associée à Γ et admettant une solution. Cette équation admet alors une solution de rang vrai nul $\gamma: \mathscr{E}_r^* \to (C \cup A_r)^*$. Si Γ' est associée à Γ par la substitution initiale $\varphi: \mathscr{E}^* \to \mathscr{E}_r^*$ déduite de $X: E \to A_r \cup 1$ (avec $XE \supset A_r$), considérons le morphisme $\alpha: \mathscr{E}^* \to (C \cup A_r)^*$ fixant les éléments de C et vérifiant: $\forall x \in E$ $\alpha x = (Xx)(\gamma x)$. On a alors $\text{alph}(\alpha\mathscr{E}) \supset C \cup XE \supset C \cup A_r$, ce qui montre que α est total. D'autre part on vérifie facilement que $\alpha e = \gamma\varphi e = \gamma f$ et $\alpha e' = \gamma\varphi e' = \gamma f'$, ce qui montre que $\alpha e = \alpha e'$ et que α est une solution de Γ. Mais toute lettre de $C \cup A_r$ figure au moins une fois au début d'un mot de $\alpha\mathscr{E}$, et donc $\text{rg}\, \Gamma \geqslant r$ d'après le Lemme 5.2, ce qui achève la preuve. □

Il est clair, à l'aide de cette dernière proposition, que l'on obtient le rang de Γ en testant si, parmi toutes les équations sur $\mathscr{E}_r$ associées à Γ (elles sont en nombre fini), l'une au moins admet une solution. En effectuant le test sur les valeurs décroissantes de r, le rang est en effet donné par la première valeur de r pour laquelle le test est positif—d'où la

Proposition 5.4. *On peut calculer le rang d'une équation dès que l'on sait décider de l'existence d'une solution d'une équation avec constantes.*

Nous allons montrer enfin que le calcul du rang d'un système fini se ramène au cas d'une équation. Pour cela nous utiliserons le lemme suivant dont la preuve est immédiate.

Lemme 5.5. *Soient u, u', v, v' quatre mots de A^+ et a, $b \notin A$. Alors $uavubv = u'av'u'bv'$ ssi $u = u'$ et $v = v'$.*

Proposition 5.6. *Soit $S = ((e_i, e_i')_{i\in[p]}, E, C)$ un système fini sur l'alphabet $\mathscr{E} = E \cup C$. On peut définir une équation $\Gamma = ((f, f'), E, C \cup C')$ (avec $\mathscr{E} \cap C' = \emptyset$) telle que les solutions (principales) de S soient exactement les restrictions à $\mathscr{E}^*$ des solutions [principales] de Γ et pour laquelle on ait l'égalité* $\operatorname{rg} \Gamma = \operatorname{rg} S$. •

Preuve. Elle s'obtient par récurrence sur p.

Soit $S = (S_1, S_2)$ un système à p équations sur l'alphabet $\mathscr{E} = E \cup C$ avec $S_1 = ((e_i, e_i')_{i=1,2}, E, C)$ et S_2 un système éventuellement vide. Soit $C' = \{a, b\}$ un alphabet disjoint de $\mathscr{E}$, $\mathscr{E}' = \mathscr{E} \cup C'$ et $(f, f') = (e_1 a e_2 e_1 b e_2,\ e_1' a e_2' e_1' b e_2')$. Montrons que les solutions (principales) de S sont les restrictions à $\mathscr{E}^*$ des solutions (principales) du système $S' = ((f, f'), S_2)$ et que l'on a l'égalité $\operatorname{rg} S = \operatorname{rg} S'$.

Si $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ est une solution du système S pour laquelle $\mathscr{A} \cap C' = \emptyset$ (ce que l'on peut toujours supposer, quitte à renommer les lettres) il est clair que le morphisme $\alpha^{\#}: \mathscr{E}'^* \to (\mathscr{A} \cup C')^*$ défini par $\alpha^{\#} = \alpha \oplus \mathrm{id}_{C'^*}$ est une solution de S' vérifiant $\operatorname{rgv} \alpha = \operatorname{rgv} \alpha^{\#}$. Réciproquement, si $\beta: \mathscr{E}'^* \to \mathscr{B}^*$ est une solution de S', le Lemme 5.5 montre que le morphisme $\beta^b: \mathscr{E}^* \to (\operatorname{alph} \beta\mathscr{E})^*$ obtenu par restriction de β est une solution du système S. L'égalité $\alpha^{\#b} = \alpha$ montre donc que les solutions de S sont les restrictions à $\mathscr{E}^*$ des solutions de S' et la relation $\operatorname{rgv} \alpha = \operatorname{rgv} \alpha^{\#}$ montre que $\operatorname{rg} S \leqslant \operatorname{rg} S'$. Montrons que $\operatorname{rg} S' \leqslant \operatorname{rg} S$.

Soit $\beta: \mathscr{E}'^* \to \mathscr{B}^*$ une solution de S' et $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ une solution de S équivalente à β^b et vérifiant $\mathscr{A} \cap C' = \emptyset$. Il est clair qu'alors $\beta' = \alpha^{\#}$ divise β. On a donc $\operatorname{rgv} \alpha^b = \operatorname{rgv} \alpha = \operatorname{rgv} \alpha^{\#} \geqslant \operatorname{rgv} \beta$ d'après la Proposition 2.2 d'où $\operatorname{rg} S \geqslant \operatorname{rg} S'$ et finalement $\operatorname{rg} S = \operatorname{rg} S'$.

Considérons maintenant une solution principale $\alpha: \mathscr{E}^* \to \mathscr{A}^*$ du système S. Quitte à renommer les lettres, on peut supposer $\mathscr{A}$ disjoint de C'. Montrons qu'alors $\alpha^{\#}$ est une solution principale de S'.

Pour cela soit $\beta: \mathscr{E}'^* \to \mathscr{B}^*$ une solution de S' divisant $\alpha^{\#}$ au moyen du

morphisme continu $\theta: \mathscr{B}^* \to (\mathscr{A} \cup C')^*$. Puisque $\theta\beta\mathscr{E} = \alpha\mathscr{E}$, on a alph θ(alph $\beta\mathscr{E}$) = alph $\alpha\mathscr{E} = \mathscr{A}$. Soit donc θ^b: (alph $\beta\mathscr{E})^* \to \mathscr{A}^*$ le morphisme obtenu par restriction de θ. Il est clair que θ^b est continu et vérifie $\alpha^{\#b} = \alpha = \theta^b\beta^b$. β^b est donc une solution de S divisant α. On a donc $\beta^b \sim \alpha$, ce qui nous permet de supposer, quitte à renommer les lettres, que l'on a alph $\beta\mathscr{E} = \mathscr{A}$ (et donc $\mathscr{B} = \mathscr{A} \cup C'$) et $\theta^b = \mathrm{id}_{\mathscr{A}^*}$. Mais puisque θ fixe les constantes, on en déduit que $\theta = \mathrm{id}_{(\mathscr{A}\cup C')^*}$ d'où $\beta \sim \alpha^{\#}$. $\alpha^{\#}$ est donc une solution principale de S'.

Réciproquement, soit $\beta: \mathscr{E}'^* \to (\mathscr{B} \cup C')^*$ une solution principale de S' (avec $\mathscr{B}$ disjoint de C'). Il est alors facile de voir que alph $\beta\mathscr{E} = \mathscr{B}$. En effet on a $\mathscr{B} \subset$ alph $\beta\mathscr{E}$ (car alph $\beta\mathscr{E}' = \mathscr{B} \cup C'$ et alph $\beta C' = C'$) et si l'on avait alph $\beta\mathscr{E} = \mathscr{B} \cup C'_0$ avec $\emptyset \neq C'_0 \subset C'$, l'utilisation d'une copie disjointe $\bar{C}'_0$ de C'_0 permettrait de définir une solution $\bar{\beta}$ divisant β et non équivalente à β obtenue à partir de β en remplaçant dans βx ($x \in E$) les occurrences des lettres de C'_0 par les lettres correspondantes de $\bar{C}'_0$. Soit donc $\beta^b: \mathscr{E}^* \to \mathscr{B}^*$ la solution de S déduite de β. Il s'agit de montrer que β^b est principale, ce qui est immédiat, puisque si α: $\mathscr{E}^* \to \mathscr{A}^*$ est une solution de S divisant β^b au moyen de θ, $\alpha^{\#}$ est une solution de S' divisant β au moyen de $\theta \oplus \mathrm{id}_{C'^*}$, d'où $\alpha^{\#} \sim \beta = \beta^{b\#}$ et finalement $\alpha \sim \beta^b$.

L'égalité $\alpha = \alpha^{\#b}$ montre donc que les solutions principales de S sont les restrictions à $\mathscr{E}^*$ des solutions principales de S', ce qui achève la preuve. □

On en déduit le corollaire suivant:

Proposition 5.7. *On sait décider de l'existence d'une solution d'un système fini et on sait calculer le rang d'un système fini dès que l'on sait décider de l'existence d'une solution d'une equation avec constantes.*

6. Conclusion

Nous avons montré que les solutions d'un système quelconque d'équations avec ou sans constantes se partitionnent en classes dont chacune admet un unique représentant qui soit une solution principale du système. La résolution d'un système se ramène donc à la recherche de ses solutions principales.

Nous avons montré également que le calcul du rang d'un système était décidable dans le cas fini et se ramenait alors au calcul du rang d'une simple équation.

Il faut cependant préciser que le calcul du rang et la solvabilité des équations avec constantes reposent sur l'algorithme de Makanin qui est pour l'instant le seul algorithme connu permettant de résoudre ces problèmes. Or cet algorithme ne peut être d'aucun secours dans la pratique et il est presque certain qu'aucun algorithme 'efficace' ne pourra jamais le remplacer. Il serait donc intéressant dans l'avenir d'étoffer la théorie des équations par la résolution ou le calcul du rang de quelques types simples d'équations avec constantes, comme cela a déjà été fait par Lentin pour les équations sans constantes.

Nous terminerons enfin avec une conjecture. Nous avons montré que tout système fini est équivalent à une simple équation. On peut en fait se demander s'il n'en serait pas de même pour un système quelconque, conjecture qui serait à rapprocher de celle des 'test sets' de [4].

Bibliographie

[1] D. Angluin, Finding patterns common to a set of strings, J. Comput. Syst. Sci. 21 (1980) 46–62.
[2] Berstel, Perrin, Perrot, Restivo, Sur le théorème du défaut, J. Algebra 60 (1) (1979).
[3] P.M. Cohn, Free Rings and Their Relations, (Academic Press, New-York/London, 1971).
[4] J. Albert, K. Culik II, Test sets for homomorphisms equivalence on context free languages, Research Report CS-79-39, Dept. of Computer Science, Waterloo (1979).
[5] Tu.I. Hmelevskii, Equations in free Semi groups, Trudy Mat. Inst. Steklov. 107 (1971). Engl. transl. Proc. Steklov Inst. Math. 107 (1971) (1976).
[6] G. Huet; Equations and rewrite rules: A survey; SRI, Tech. Rep. CSL-III (1980).
[7] A. Lentin, Equations dans les monoïdes libres (Gauthier-Villars, Paris, 1972).
[8] A. Lentin, Equations in free monoïds, in: M. Nivat, ed., Automata, Languages and Programming, (North Holland, Amsterdam, 1972 67–85).
[9] A. Lentin and M.P. Schützenberger, A combinatorial problem in the theory of free monoïds, Proc. University of North-Carolina 128–144 (1967).
[10] Lothaire, Combinatorics on words (Addison Wesley, Reading, MA, 1982).
[11] R.C. Lyndon, Equations in free groups, Trans. Amer. Math. Soc. 96 (1960) 445–457.
[12] R.C. Lyndon and P.E. Schupp, Combinatorial Group Theory (Springer, Berlin, 1977).
[13] G.S. Makanin, The problem of solvability of equations in a free semigroup, Math. USSR Sbornik 32 (2) (1977); in: Am. Math. Soc. (1978).
[14] G.S. Makanin, Algorithmic decidability of the rank of constant free equations in a free semigroup, Dokl. Akad. Nauk. SSSR 243 (1978).
[15] J.P. Pécuchet, Sur la détermination du rang d'une équation dans le monoïde libre, Theor. Comput. Sci. 16, (1981) 337–340.
[16] J.P. Pécuchet, Equations avec constantes et algorithme de Makanin, Thèse de 3-ième Cycle (1981), Rouen.
[17] G. Rozenberg and A. Salomaa, The Mathematical Theory of *L* Systems (Academic Press, New-York/London, 1980).
[18] G.S. Makanin, On the rank of equations in four unknowns in a free semigroup, Mat. Sb. 103 (1977) 147–236. (English translation: Math. USSR Sb. 29 (1977) 257–280.)